(12)特許協力条約に基づいて公開された国際出願

542 888

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年8 月5 日 (05.08.2004)

PCT

(10) 国際公開番号
WO 2004/066177 A1

(51) 国際特許分類[7]: G06F 17/60

(21) 国際出願番号: PCT/JP2003/000473

(22) 国際出願日: 2003 年1 月21 日 (21.01.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 三井物産株式会社 (MITSUI & CO., LTD.) [JP/JP]; 〒100-0004 東京都 千代田区 大手町一丁目２番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 大島 俊一 (OSHIMA,Shunichi) [JP/JP]; 〒100-0004 東京都 千代田区 大手町一丁目２番１号 三井物産株式会社内 Tokyo (JP). 斎藤 晃 (SAITO,Hikaru) [JP/JP]; 〒100-0004 東京都 千代田区 大手町一丁目２番１号 三井物産株式会社内 Tokyo (JP). 奈良原 智明 (NARAHARA,Tomoaki) [JP/JP]; 〒100-0004 東京都 千代田区 大手町一丁目２番１号 三井物産株式会社内 Tokyo (JP). 中里 昇吾 (NAKAZATO,Shogo) [JP/JP]; 〒100-0004 東京都 千代田区 大手町一丁目２番１号 三井物産株式会社内 Tokyo (JP). 吉川 治宏 (KIKKAWA,Haruhiro) [JP/JP]; 〒101-0052 東京都 千代田区神田小川町 3－3－2 マツシタビル 三井物産デジタル株式会社内 Tokyo (JP). 荻猛 (OGI,Takeshi) [JP/JP]; 〒101-0052 東京都 千代田区神田小川町 3－3－2 マツシタビル 三井物産デジタル株式会社内 Tokyo (JP).

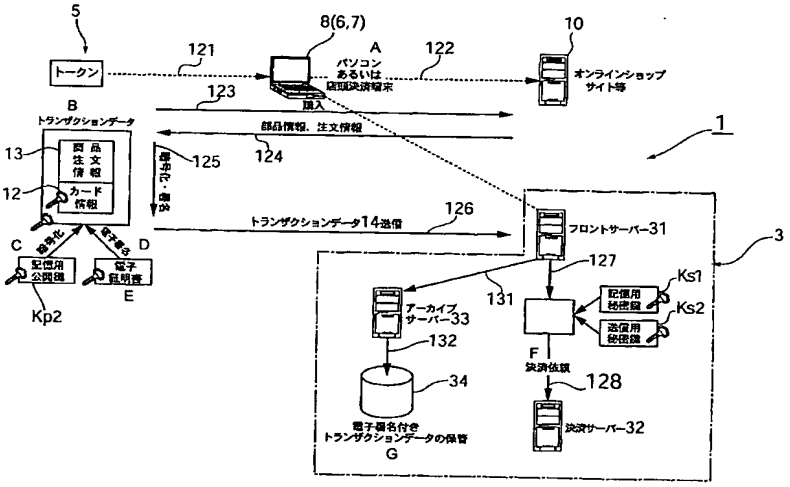
(74) 代理人: 市原 俊一, 外 (ICHIHARA,Shunichi et al.); 〒160-0004 東京都 新宿区 四谷２丁目８番地 コーポクローバ浜５０５号 Tokyo (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK,

[続葉有]

(54) Title: CARD SETTLEMENT METHOD USING PORTABLE ELECTRONIC DEVICE HAVING FINGERPRINT SENSOR

(54) 発明の名称: 指紋センサ付き携帯型電子機器を用いたカード決済方法



5...TOKEN
A...PERSONAL COMPUTER OR SHOP SETTLEMENT TERMINAL
10...ONLINE SHOT SITE OR THE LIKE
123...PURCHASE
124...PARTS INFORMATION, ORDER INFORMATION
B...TRANSACTION DATA
13...COMMODITY ORDER INFORMATION
12...CARD INFORMATION
C...ENCRYPTION
D...ELECTRONIC SIGNATURE
Kp2...STORAGE PUBLIC KEY
E...ELECTRONIC CERTIFICATE
125...ENCRYPTION, SIGNATURE
126...TRANSACTION DATA 14 TRANSMISSION
31...FRONT SERVER
33...ARCHIVE SERVER
Ks1...STORAGE SECRET KEY
Ks2...TRANSMISSION SECRET KEY
F...SETTLEMENT REQUEST
G...STORAGE OF TRANSACTION DATA HAVING ELECTRONIC SIGNATURE
32...SETTLEMENT SERVER

(57) Abstract: In a card settlement system using a portable electronic device having a fingerprint sensor, a credit card and a portable electronic device (5) having a fingerprint sensor are issued to a person who has made application. To this electronic device (5), card information (12), a storage public key Kp1, and

[続葉有]

WO 2004/066177 A1

DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

a transmission public key Kp2 are assigned. When registering the electronic device (5) to be usable, a card management device (3) is accessed to identify an individual and when a registration permission signal is received, master fingerprint data (11) can be registered by a fingerprint sensor (51). The fingerprint data entered at this registration is used to create individual encryption keys Ks3, Kp3. Upon card settlement, the fingerprint is checked for authentication. Commodity order information (13) and card information (12) are encrypted by the transmission public key Kp2 and electronically signed by the individual encryption key Ks3. Transaction data (14) having the electronic signature is transmitted to a card management apparatus (3) where the data is decrypted and card settlement is performed.

(57) 要約: 指紋センサ付き携帯型電子機器を用いたカード決済システム（１）では、カード申し込み者にクレジットカードと共に指紋センサ付き携帯型電子機器（５）を発行する。この電子機器（５）には、カード情報（１２）と共に記憶用公開鍵Ｋｐ１および送信用公開鍵Ｋｐ２が付与されている。電子機器（５）を利用可能にするための登録時に、カード管理装置（３）にアクセスして、個人確認を行い登録許可信号を受信すると、指紋センサ（５１）によるマスター指紋データ（１１）の登録が可能になる。この登録時の指紋データを利用して個人用暗号鍵Ｋｓ３、Ｋｐ３が生成される。カード決済時には、指紋照合により本人確認が行われる。商品注文情報（１３）、カード情報（１２）が、送信用公開鍵Ｋｐ２によって暗号化され、個人用暗号鍵Ｋｓ３によって電子署名される。かかる電子署名付きのトランザクションデータ（１４）がカード管理装置（３）に送信され、復号化されてカード決済処理が行われる。

明細書

指紋センサ付き携帯型電子機器を用いたカード決済方法

技術分野

本発明は、ネットワーク上で注文した商品等の購入代金をカード決済するために用いる指紋センサ付き携帯型電子機器に関するものである。また、指紋センサ付き携帯型電子機器を用いて、ネットワーク上で注文した商品等の購入代金のカード決済を安全に行うためのカード決済方法に関するものである。

背景技術

クレジットカード、デビットカードなどの決済用カードを用いて、商品代金やサービス料を支払う場合、カード使用者が本当にカード所有者であるか否かを確認する必要がある。この本人確認は、店頭でカード使用者の運転免許証やパスポートなどの身分証明書を確認すること以外にない。ここで、一部の決済用カードにはカード所有者の顔写真がプリントされている。この場合には、決済用カードにプリントされている顔写真とカード使用者とを照合することにより、本人確認を行うことが可能である。

カード決済時の本人確認は、店頭で店員がカード使用者と対面している場合には、上記のように、身分証明書や決済用カードにプリントされている顔写真により行うことが可能である。しかし、例えばインターネット上での商品代金やサービス料の支払の場合、あるいは、店員が介在しないカード決済端末を使用する場合（例えば、給油所のポンプに内蔵されているカード決済端末などを使用する場合）には、カード使用者が本当にカード所有者であるか否かを確認

することが大変困難である。

インターネットなどのネットワーク上において決済用カードによる決済を行う場合、一般的には、カード番号とカード所有者の名前および有効期限を入力するだけで決済が完了する場合が殆どである。しかしながら、次のようなカード決済に絡む問題が跡を絶たないのが現状である。

1） 第三者が他人のカード番号を何らかの方法で知り、それを利用して、インターネット上で商品の購入を行う、所謂、なりすましの問題

2） カード所有者がインターネット上で商品の購入を行っているにも拘わらず、購入していないと白を切る取引否認の問題

従来においては、このような問題を解決するために次のような方法が採用あるいは提案されている。

まず、ビザインターナショナルでは、インターネット上での決済を安全に行う手段として、「３－Ｄ　Ｓｅｃｕｒｅ」と呼ばれる方法を提案している。この方法では、カード所有者各々が自分で決めたパスワードや、本人を特定する秘密の質問（ペットの名前や母親の旧姓など）を、カード会社のサーバーに登録しておく。インターネット上でカード所有者に商品の販売やサービスの提供を行う業者は、カード会社のサーバー上に予め登録されている登録データに関する質問を購入者に行い、購入者が本当にカード所有者であるか否かを確認する。

しかしながら、この方法を用いても、カード番号、パスワード、秘密の質問に対する回答を「生のまま」パーソナルコンピュータに入力することに変わりは無い。このため、入力されたこれらのデータを、何らかの方法で知り得た悪意の第三者による「なりすまし」

を完全に防御出来ない。また、この方法は、パーソナルコンピュータを介したインターネット上のカード決済の場合には実行出来るが、給油所のポンプなどに設置されているカード決済端末のように、人間が全く介在しないカード決済端末を利用する場合には適用出来ない。

次に、米国特許第６，１０５，００８号および同６，２８２，５２２号（ビザインターナショナル）では、所謂スマートＩＣカードを用いたカード決済方法において、同ＩＣカードに事前に使用可能金額を登録しておき、その金額の範囲でしかインターネット上での買い物が出来ないようにする方法が提案されている。しかし、この方法では、利用者は毎回残存金額を確認したり、金額を追加するなどの手間がかかるという問題がある。また、カードを紛失した場合やカードが盗まれた場合、第三者によるカードの不正使用の危険性を排除することができない。

ここで、インターネットにおける安全な決済方法として指紋を利用したものが提案されている。例えば、米国特許出願公開第２００２／００１８５８５号公報に開示されている方法では、利用者自身の指紋データそのものを、クレジットカード番号などのデータ暗号化の鍵として使用している。しかしながら、この方法では、利用者は自身の指紋データをネットワーク上のサーバーに登録しなければならず、利用者の心理的な抵抗が大きい。また、店頭におけるカード決済端末においても端末に付随した指紋スキャナーで指紋をスキャンし、同データが毎回ネットワーク上に送信されるなど、一般の消費者が指紋に対して抱いているイメージを考慮していない方式と言える。

同様に、米国特許出願公開第２００１／０００００５３５号公報に開示されている方法においても、利用者本人の指紋データをネット

ワーク上のサーバーに登録しておくことを前提としている。

発明の開示

本発明の目的は、ネットワーク上でのカード決済時における本人確認を正確かつ安全に行うことにより、第三者によるカード不正使用を確実に防止可能なカード決済方法を提案することにある。具体的には、本人確認手段として指紋認証を用い、認証された本人のみが、ネットワーク上に指紋情報を含む本人情報が流出しない状態でカード決済を行うことができ、簡便で高度なセキュリティー手段により決済情報の秘匿性を確保可能であり、さらに、本人自体もカード番号やパスワードを知る必要が無いので強固なセキュリティーを期待できる、カード決済方法を提案することにある。

また、本発明の目的は、ネットワーク上でのカード決済時に、カード所有者本人による取引行為であることを明確化し、カード所有者による決済取引の否認などの問題を解消することのできるカード決済方法を提案することにある。

さらに、本発明の目的は、ネットワーク上でのカード決済を安全に行うためのカード決済方法に用いるに適した指紋センサ付き携帯型電子機器を提案することにある。

上記の目的を達成するために、本発明は、指紋センサ付き携帯型電子機器を、通信端末を介して、カード会社のカード管理装置に接続し、商品購入代金などのカード決済を行うカード決済方法であって、

前記指紋センサ付き携帯型電子機器において、前記指紋センサにより利用者の指紋を読み取らせ、予め登録されている指紋データと照合することにより、利用者が前記指紋センサ付き携帯型電子機器の所有者であるか否かの本人確認を行う本人確認工程と、

前記指紋センサ付き携帯型電子機器において、本人確認が行われた場合に、商品注文情報と、予め登録されているカード情報とを、予め登録されている送信用公開鍵によって暗号化して送信データを生成すると共に、予め登録されている個人用暗号鍵によって前記送信データに電子署名を行う送信データの生成・署名工程と、

前記指紋センサ付き携帯型電子機器の側から、前記電子署名付きの送信データを前記カード管理装置に送信する送信工程と、

前記カード管理装置において、前記電子署名付きの送信データを、前記送信用公開鍵とペアとなっている送信用秘密鍵を用いて復号化して、決済処理を行う工程と、

を含むことを特徴としている。

ここで、前記指紋センサ付き携帯型電子機器の前記指紋データおよび前記カード情報は、前記カード管理装置の側から付与された記憶用公開鍵によって暗号化された状態で登録されていることが望ましい。この場合、前記カード管理装置における前記カード決済用データを復号化する工程では、前記記憶用公開鍵とペアとなっている記憶用秘密鍵を用いて復号化を行えばよい。

また、前記カード管理装置は、受信した前記カード決済用データを所定期間、記憶保持することが望ましい。

次に、必要に応じて、前記カード管理装置が、前記指紋センサ付き携帯型電子機器に登録されている前記送信用公開鍵および前記記憶用公開鍵を更新することが望ましい。この場合、前記指紋センサ付き携帯型電子機器は、登録されている前記カード情報および前記指紋データを、更新後の前記記憶用公開鍵を用いて暗号化した前記カード情報および前記指紋データに書き換える処理を行えば良い。

一方、本発明は、通信端末を介して、カード会社のカード管理装置に接続して、商品購入代金などのカード決済を行うために用いる

指紋センサ付き携帯型電子機器であって、

指紋センサと、記憶部と、前記通信端末に接続するための外部インターフェースと、各部を駆動制御するためのプロセッサとを有し、

前記記憶部には、前記カード管理装置の側から付与された送信用公開鍵および記憶用公開鍵と、当該指紋センサ付き携帯型電子機器の所有者に付与された決済用カードのカード情報と、マスター指紋データと、個人用暗証鍵とが記憶されており、

前記カード情報および前記マスター指紋データは、前記記憶用公開鍵によって暗号化された状態で記憶されており、

前記プロセッサは、

前記指紋センサによる前記マスター指紋データの読取時に前記個人用暗証鍵を生成する個人用暗号鍵生成手段と、

前記指紋センサによって読み取った指紋を前記記憶部の前記指紋データと照合することにより本人確認を行う本人確認手段と、

前記送信用公開鍵を用いて商品注文情報および前記カード情報を暗号化して送信データを生成すると共に、前記個人用暗号鍵を用いて前記送信データに電子署名を行い、前記電子署名付きの送信データを、前記カード管理装置に向けて送信する送信データ生成・送信手段とを備えていることを特徴としている。

ここで、前記プロセッサは、前記カード管理装置から登録許可信号を受信すると、前記指紋センサによる前記マスター指紋データの読み取りおよび登録を行わせるマスター指紋データ登録手段を備えた構成とすることができる。この場合、前記個人用暗号鍵生成手段は、前記マスター指紋データの読み取り時に読み取られた指紋データを利用して、前記個人用暗号鍵を生成することが望ましい。

次に、本発明は、指紋センサ付き携帯型電子機器から、通信端末を介して受信するカード決済用データに基づき、商品購入代金など

のカード決済を行うためのカード管理装置であって、

前記指紋センサ付き携帯型電子機器に付与される記憶用公開鍵および送信用公開鍵を生成する暗号鍵生成手段と、

前記指紋センサ付き携帯型電子機器から登録要求信号を受信すると、利用者を特定するための身元識別情報を要求し、受信した身元識別情報に基づき利用者を特定した場合に、登録許可信号を前記指紋センサ付き携帯型電子機器に向けて送信する登録手続き処理手段と、

前記指紋センサ付き携帯型電子機器から暗号化された前記カード決済用データを受信すると、前記記憶用公開鍵とペアとなっている記憶用秘密鍵と、前記送信用公開鍵とペアとなっている送信用秘密鍵とを用いて、前記カード決済用データを復号化する復号化手段と、

復号化された前記カード決済用データに基づき、決済処理を行う決済処理手段とを有していることを特徴としている。

一方、本発明は、指紋センサ付き携帯型電子機器を、通信端末を介して、カード会社のカード管理装置に接続し、商品購入代金などのカード決済を行うカード決済システムであって、

前記指紋センサ付き携帯型電子機器は、

前記指紋センサにより利用者の指紋を読み取らせ、予め登録されている指紋データと照合することにより、利用者が前記指紋センサ付き携帯型電子機器の所有者であるか否かの本人確認を行う本人確認手段と、

本人確認が行われた場合に、商品注文情報と、予め登録されているカード情報とを、予め登録されている送信用公開鍵によって暗号化して送信データを生成すると共に、予め登録されている個人用暗号鍵によって前記送信データに電子署名を行う送信データの生成・署名手段と、

前記電子署名付きの送信データを前記カード管理装置に送信する送信手段とを備えており、

前記カード管理装置は、

前記電子署名付きの送信データを受信する受信手段と、

受信した前記電子署名付きの送信データを、前記送信用公開鍵とペアとなっている送信用秘密鍵を用いて復号化する復号化手段と、

復号化された前記電子署名付きの送信データに基づき、決済処理を行う決済処理手段とを備えていることを特徴としている。

ここで、前記指紋センサ付き携帯型電子機器の前記指紋データおよび前記カード情報は、前記カード管理装置の側から付与された記憶用公開鍵によって暗号化された状態で登録されており、前記カード管理装置の前記復号化手段は、前記記憶用公開鍵とペアとなっている記憶用秘密鍵を用いて復号化を行うことが望ましい。

また、前記カード管理装置は、受信した前記カード決済データを所定期間、記憶保持する記憶手段を備えていることが望ましい。

さらに、前記カード管理装置は、前記指紋センサ付き携帯型電子機器に登録されている前記送信用公開鍵および前記記憶用公開鍵を更新する暗号鍵更新手段を備えていることが望ましい。この場合、前記指紋センサ付き携帯型電子機器は、登録されている前記カード情報および前記指紋データを、更新後の前記記憶用公開鍵を用いて暗号化した前記カード情報および前記指紋データに書き換えるデータ更新手段を備えていることが望ましい。

図面の簡単な説明

図１は、本発明を適用したカード決済システムを示す概略構成図である。

図２は、図１の指紋センサ付き携帯型電子機器の概略ブロック図

である。

図３は、図１のカード決済システムにおける登録手続きを示すための説明図である。

図４は、図１のカード決済システムにおけるカード決済手続きを示すための説明図である。

発明を実施するための最良の形態

以下に、図面を参照して、本発明のカード決済方法を適用したカード決済システムの実施例を説明する。

（システム構成）

図１は本例のカード決済システムを示す概略構成図であり、図２は指紋センサ付き携帯型電子機器の概略ブロック図である。カード決済システム１は、カード会社２の側に設置されているカード管理装置３と、カード管理会社２からクレジットカードなどの決済用カードの所有者４に提供された指紋センサ付き携帯型電子機器５と、指紋センサ付き携帯型電子機器５を接続可能なパーソナルコンピュータ６やカード決済端末７などの通信端末８とを有している。また、指紋センサ付き携帯型電子機器５およびカード管理装置３の間を接続可能なネットワーク、例えばインターネット９とを有している。

指紋センサ付き携帯型電子機器５は、カード会社２が、カード申し込み者に対してクレジットカードと共に発行される。カード申し込み者は、指紋センサ付き携帯型電子機器５を受け取ると、通信端末８およびインターネット９を介してカード会社２のカード管理装置３にアクセスして、クレジットカード利用のための登録手続きを行う。登録手続きが完了すると、指紋センサ付き携帯型電子機器５を用いて、インターネット９上におけるオンラインショップサイト１０などで購入した商品の代金を、カード決済により支払うことが

可能になる。

指紋センサ付き携帯型電子機器５は、指紋センサ５１と、指紋データの抽出と照合を行うプロセッサ５２と、指紋データおよびその他のデータを保管する不揮発性メモリ５３と、通信端末８と通信を行うための外部インターフェース５４とを有している。

不揮発性メモリ５３には、カード情報を暗号化して保管するための公開鍵（以下、記憶用公開鍵と呼ぶ。）Ｋｐ１と、暗号化されたカード情報を更に暗号化してカード管理装置３に送信するための公開鍵（以下、送信用公開鍵と呼ぶ。）Ｋｐ２が書き込まれている。また、指紋データを利用して生成されたカード所有者自身の秘密鍵Ｋｓ３と公開鍵Ｋｐ３が書き込まれている。例えば、指紋データのノイズを利用してこのような秘密鍵および公開鍵を生成することができる。さらに、カード所有者のマスター指紋データ１１が登録されている。

一方、カード会社２のカード管理装置３は、ウェブサーバーであるフロントサーバー３１と、決済サーバー３２と、アーカイブサーバー３３と、カード決済履歴などを保管するデータベース３４とを備えている。フロントサーバー３１は、インターネット９を介して受信した情報を復号化して決済サーバー３２へ渡すためのものである。フロントサーバー３１は、指紋センサ付き携帯型電子機器５が保持している送信用公開鍵Ｋｐ２とペアになる送信用秘密鍵Ｋｓ２と、記憶用公開鍵Ｋｐ１とペアになる記憶用秘密鍵Ｋｓ１を保持しており、これらの秘密鍵Ｋｓ１、Ｋｓ２を用いて受信した情報を復号化する。なお、本例では、全ての公開鍵、暗号鍵、電子署名の方式はＰＫＩ．Ｘ．５０９の仕様に準拠している。

（登録手続き）

本例のカード決済システム１の利用に先立って、指紋センサ付き

携帯型電子機器５の発行および登録手続きが必要である。図３を参照して、この手続きを説明する。

まず、クレジットカードの申し込み者がカード会社２に対してカード申し込み手続きを郵送あるいはオンラインにより行うと（矢印１０１）、カード会社２は、指紋センサ付き携帯型電子機器（トークン）５とクレジットカードを申し込み者に発行する（矢印１０２）。

カード会社２が指紋センサ付き携帯型電子機器５を発行する際には、カード会社２は指紋センサ付き携帯型電子機器５の不揮発性メモリ５３に次の情報を書き込む。

１）カード情報を暗号化して保管するための記憶用公開鍵Ｋｐ１

２）暗号化されたカード情報を更に暗号化して送るための送信用公開鍵Ｋｐ２

３）カード情報１２

申し込み者は、カード会社２から指紋センサ付き携帯型電子機器５とクレジットカードを受け取り次第、指紋センサ付き携帯型電子機器５をパーソナルコンピュータ６などの通信端末８に接続する（矢印１０３）。そして、通信端末８およびインターネット９を介して、カード会社２から指定されたＵＲＬにアクセスし、カード管理装置３のフロントサーバー３１との通信を確立し（矢印１０４）、登録要求信号（アクティベーション要求）を出す（矢印１０５）。

この後は、カード申し込み時に申し込み者が記入した社会保険番号や運転免許証番号の問合せ、および、秘密の質問（ペットの名前、母親の旧姓など）がウェブ上でなされ（身元識別情報の確認）、本人確認が行われる（矢印１０６）。当該質問において、カード会社のフロントサーバー３１が回答入力者をカード申し込み者本人であることを確認できると、カード会社２のフロントサーバー３１は、指紋センサ付き携帯型電子機器５に対して指紋データ登録開始を許

可する登録許可信号（アクティベーション許可信号）を送る（矢印１０７）。これにより、カード申し込み者は、カード会社２の側において、カード会員４として正式に登録される。

アクティベーション許可信号を受信した通信端末８の画面上には、「指紋センサ付き携帯型電子機器へ指を載せて下さい」とメッセージが表示される。カード会員４がメッセージに従って指を指紋センサによってスキャンさせる。数本の指について指紋の登録を行うため、同様の指示が繰り返される（ブロック１０８）。

指紋センサ付き携帯型電子機器５は、必要とされる指紋データが揃ったことを確認すると、同指紋データを、マスター指紋データ１１として、不揮発性メモリに登録する（矢印１０９）。同時に、指紋データを利用して、カード会員４の個人用秘密鍵Ｋｓ３と個人用公開鍵Ｋｐ３を生成する。例えば、指紋データの取得時における指紋データに乗っているノイズを利用して、カード会員４の個人用秘密鍵Ｋｓ３と個人用公開鍵Ｋｐ３を生成する。これらの鍵は電子証明書の作成に利用される。

（カード決済手続き）

次に、図４を参照して、本例のカード決済システム１におけるインターネット上でのカード決済手続きを説明する。

カード会員４がインターネット９上で商品の購入やサービスの提供を受ける際には、指紋センサ付き携帯型電子機器５を通信端末８に接続し（矢印１２１）、通信端末８を介してオンラインショッピングサイト１０にアクセスする（矢印１２２）。通信端末８を介して商品購入を行うと（矢印１２３）、オンラインショッピングサイト１０側から商品情報および注文情報が返信される（矢印１２４）。

注文商品の購入代金の決済時には、決済用のカード番号を入力する代りに、指紋センサ付き携帯型電子機器（トークン）５の指紋セ

ンサ５１により、登録されている指紋に対応する指をスキャンする。不揮発性メモリー５３に記憶されているマスター指紋データ１１と、スキャンされた指の指紋データが一致すると、指紋センサ付き携帯型電子機器５は、カード会員４が決済行為を行っていると認識し、カード会社２によって書き込まれた記憶用暗号鍵Ｋｐ１で暗号化されたカード情報１２と購入する商品に関する情報（商品注文情報）１３を、送信用暗号鍵Ｋｐ２で暗号化する。同時に、カード会員４の個人用公開鍵Ｋｐ３および秘密鍵Ｋｓ３で電子署名をする（矢印１２５）。そして、暗号化され、電子署名がなされた送信データ（電子署名つきトランザクションデータ）１４をインターネット９を介してカード会社２のフロントサーバー３１に送信する（矢印１２６）。ここで、電子署名を行う意味は、カード会員４によるカード決済行為の否認を防止するためである。

電子署名つきトランザクションデータ１４をカード会社２のフロントサーバー３１が受信すると、送信用暗号鍵Ｋｐ２とペアである秘密鍵Ｋｓ２で復号化し、更に、記憶用暗号鍵Ｋｐ１とペアである秘密鍵Ｋｓ１で復号化し、カード情報１２を復号化する（ブロック１２７）。そして、決済サーバー３２に決済依頼を行う（矢印１２８）。すなわち、従来と同様の決済プロセスへ処理を渡す。また、カード会員４による決済行為の否認などの防犯上の理由から、送られてきた電子署名付きのトランザクションデータ１４を長期アーカイブすることも可能である（矢印１３１、１３２）。

このように、本例のカード決済システム１では、指紋センサ付き携帯型電子機器５内で生成された個人の秘密鍵Ｋｓ３により電子署名を行うことによって、登録した指紋の持ち主であるカード会員本人が指紋センサ付き携帯型電子機器５を使用し決済行為を行ったことが特定される。また、同暗号化データを、カード会社２のフロン

トサーバー３１の秘密鍵Ｋｓ１、Ｋｓ２で復号化することにより、データ自体がカード会社発行の指紋センサ付き携帯型電子機器５から送信されたことが特定される。

この二点から、カード決済を行った人間の特定を確実に行うことができ、使用された指紋センサ付き携帯型電子機器５の真偽の判断を確実に行うことができる。よって、カード会社２にとって非常に安全性の高いネットワーク決済方法を実現できる。

ここで、指紋センサ付き携帯型電子機器５が、パーソナルコンピュータ６などの通信端末８を介してインターネット９に接続される場合は、カード会社２の決済サーバー３２とオンラインで通信する。よって、必要の都度、カード会社２は指紋センサ付き携帯型電子機器５に書き込まれている記憶用公開鍵Ｋｐ１および送信用公開鍵Ｋｐ２を変更することが可能である。このようにすれば、暗号化の為に用いる暗号鍵のセキュリティを更に高めることが出来る。なお、暗号鍵を書き換えた場合には、不揮発性メモリ５３に書き込まれているデータを、新しい暗号鍵を用いて暗号化したデータによって更新する必要がある。

次に、上記の例は、インターネット経由での商品などの購入時の代金決済手続きである。本例のカード決済システム１は、通常のカード決済による商品・サービスの購入であっても、例えば給油所のカード決済端末７のような、人間を介在しないカード使用の場合にも用いることができる。この場合には、電子機器５を給油所のポンプのカード決済端末７に接続することにより、利用者を特定でき、また、カード決済行為の電子署名を行うことができ、さらには、指紋センサ付き携帯型電子機器５の真偽の判別も行うことができる。

産業上の利用の可能性

以上説明したように、本発明の指紋センサ付き携帯型電子機器を用いたカード決済方法では、当該電子機器の内部に登録されているカード会員の指紋データが外部に一切出力されない。指紋データは、カード会員本人かどうかを、当該電子機器が認識する為に使用されるのみであり、当該電子機器に記憶されているカード番号などの決済に必要な情報を暗号化する鍵は、同カード発行会社が任意に決定でき、また、随時変更登録可能である。よって、カード会員およびカード会社の双方にとって、より安全で、利便性が高く、且つカード会員のプライバシーを尊重したカード決済方法を実現できる。

すなわち、本発明によれば、次のような作用、効果が得られる。

1） カード会員本人の指紋と一致しない限り、カード情報に係わるデータが、カード会社のサーバーに送信されない。また、指紋センサ付き携帯型電子機器に保持されているカード会員個人の秘密鍵を利用して電子署名が行われる。

よって、必ずカード会員自身からの決済要求であることをカード会社が確認でき、第三者によるなりすましを防止できる。また、カード会員自身がカード決済を行ったのに、行っていないと嘘をつくこと（否認）もできない。

2） カード会員本人が自分のカード番号を知る必要がないため、カード会員本人の人為的ミスでカード番号が他人に漏れる心配がない。

3） 指紋センサ付き携帯型電子機器から出力されるカード情報に係わるデータは、常にカード会社が事前に当該電子機器に書き込んだ（カード会社のサーバーの秘密鍵とペアとなっている）公開鍵によって暗号化されて出力される。同時に、カード会員個人の秘密鍵で電子署名が行われる。従って、何らかの方法でデータが盗まれ、あるいは改竄されたとしても、悪用されることが無い。

4） カード番号などの「生のカード情報」は、指紋センサ付き携帯型電子機器のメモリに、カード会社が事前に当該電子機器に書き込んだ公開鍵で暗号化されて記憶されている。また、当該電子機器外部へは更に暗号化されないと出力されない。従って、カード情報を、高い安全性を持って保管出来る。

万一、指紋センサ付き携帯型電子機器を紛失しても、カード会員本人の指紋データと一致しない限り当該電子機器は使用出来ず、また記憶されているカードデータは暗号化されている。従って、紛失し、あるいは盗難にあった指紋センサ付き携帯型電子機器が使用される危険も少ない。また、不正な方法でデータを取り出そうとした場合、自己破壊機能（所謂、Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｔ）と組み合わせることにより、より安全な運用が可能である。

5） 「生のカード情報」と同様、カード会員自身の登録指紋データも指紋センサ付き携帯型電子機器の内部にのみ記憶され、当該電子機器の外部へ出力されることは一切ない。従って、個人のセキュリティー保持の観点からもカード会員にとって受け入れ易く、好ましい。

6） カード会社は既存の決済サーバーの前面にＰＫＩ方式の暗号鍵サーバーであるフロントサーバーを追加するだけで、本発明によるカード決済方法を利用できるので、既存の決済システムの変更が極めて少ない。

7） 指紋センサ付き携帯型電子機器に、パーソナルコンピュータへの接続用インターフェース機能と共に、既存のカード決済端末とワイヤレス（電磁波、赤外線など）で通信出来る機能を付加した場合には、本発明のカード決済方法の適用範囲を広げることができる。すなわち、インターネットの決済以外でも、従来においてカード会員の使用かどうかを特定することが極めて困難であった無人店舗の

カード決済端末などにおいて、決済端末側に無線の受信部を追加するだけで、本発明のカード決済方法を利用でき、インターネット上の決済と同様の既存問題を解決することができる。

8） カード会社が必要の都度、指紋センサ付き携帯型電子機器の内部に記憶したカード情報を暗号化する為の暗号鍵をオンラインで書き換えるようにした場合には、当該電子機器とカード会社の決済サーバー間の高いセキュリティーを保持できる。

請求の範囲

1. 指紋センサ付き携帯型電子機器を、通信端末を介して、カード会社のカード管理装置に接続し、商品購入代金などのカード決済を行うカード決済方法であって、

前記指紋センサ付き携帯型電子機器において、前記指紋センサにより利用者の指紋を読み取らせ、予め登録されている指紋データと照合することにより、利用者が前記指紋センサ付き携帯型電子機器の所有者であるか否かの本人確認を行う本人確認工程と、

前記指紋センサ付き携帯型電子機器において、本人確認が行われた場合に、商品注文情報と、予め登録されているカード情報とを、予め登録されている送信用公開鍵によって暗号化してトランザクションデータを生成すると共に、予め登録されている個人用暗号鍵によって電子署名を行うトランザクションデータの生成・署名工程と、

前記指紋センサ付き携帯型電子機器の側から、前記電子署名付きのトランザクションデータを前記カード管理装置に送信する送信工程と、

前記カード管理装置において、前記電子署名付きのトランザクションデータを、前記送信用公開鍵とペアとなっている送信用秘密鍵を用いて復号化して、決済処理を行う工程と、

を含むことを特徴とする指紋センサ付き携帯型電子機器を用いたカード決済方法。

2. 請求の範囲第1項において、

前記指紋センサ付き携帯型電子機器の前記指紋データおよび前記カード情報は、前記カード管理装置の側から付与された記憶用公開鍵によって暗号化された状態で登録されており、

前記カード管理装置における前記電子署名付きのトランザクションデータを復号化する工程では、前記記憶用公開鍵とペアとなっている記憶用秘密鍵を用いた復号化工程も含まれていることを特徴とする指紋センサ付き携帯型電子機器を用いたカード決済方法。

3. 請求の範囲第1項または第2項において、

前記カード管理装置は、受信した前記電子署名付きのトランザクションデータを所定期間、記憶保持することを特徴とする指紋センサ付き携帯型電子機器を用いたカード決済方法。

4. 請求の範囲第1項、第2項または第3項において、

前記カード管理装置が、前記指紋センサ付き携帯型電子機器に登録されている前記送信用公開鍵および前記記憶用公開鍵を更新する工程を含み、

前記指紋センサ付き携帯型電子機器は、登録されている前記カード情報および前記指紋データを、更新後の前記記憶用公開鍵を用いて暗号化した前記カード情報および前記指紋データに書き換えることを特徴とする指紋センサ付き携帯型電子機器を用いたカード決済方法。

5. 通信端末を介して、カード会社のカード管理装置に接続して、商品購入代金などのカード決済を行うために用いる指紋センサ付き携帯型電子機器であって、

指紋センサと、記憶部と、前記通信端末に接続するための外部インターフェースと、各部を駆動制御するためのプロセッサとを有し、

前記記憶部には、前記カード管理装置の側から付与された送信用公開鍵および記憶用公開鍵と、当該指紋センサ付き携帯型電子機器

の所有者に付与された決済用カードのカード情報と、マスター指紋データと、個人用暗証鍵とが記憶されており、

前記カード情報および前記マスター指紋データは、前記記憶用公開鍵によって暗号化された状態で記憶されており、

前記プロセッサは、

前記指紋センサによる前記マスター指紋データの読取時に前記個人用暗証鍵を生成する個人用暗号鍵生成手段と、

前記指紋センサによって読み取った指紋を前記記憶部の前記指紋データと照合することにより個人確認を行う個人確認手段と、

前記送信用公開鍵を用いて商品注文情報および前記カード情報を暗号化してトランザクションデータを生成すると共に、前記個人用暗号鍵を用いて電子署名を行い、電子署名付きの前記トランザクションデータを前記カード管理装置に向けて送信するトランザクションデータの生成・送信手段とを備えていることを特徴とするカード決済に用いる指紋センサ付き携帯型電子機器。

6. 請求の範囲第5項において、

前記プロセッサは、前記カード管理装置から登録許可信号を受信すると、前記指紋センサによる前記マスター指紋データの読み取りおよび登録を行わせるマスター指紋データ登録手段を備えており、

前記個人用暗号鍵生成手段は、前記マスター指紋データの読み取り時に読み取られた指紋データを利用して、前記個人用暗号鍵を生成することを特徴とするカード決済に用いる指紋センサ付き携帯型電子機器。

7. 指紋センサ付き携帯型電子機器から、通信端末を介して受信するトランザクションデータに基づき、商品購入代金などのカ

ード決済を行うためのカード管理装置であって、

前記指紋センサ付き携帯型電子機器に付与される記憶用公開鍵および送信用公開鍵を生成する暗号鍵生成手段と、

前記指紋センサ付き携帯型電子機器から登録要求信号を受信すると、利用者を特定するための身元識別情報を要求し、受信した身元識別情報に基づき利用者を特定した場合に、登録許可信号を前記指紋センサ付き携帯型電子機器に向けて送信する登録手続き処理手段と、

前記指紋センサ付き携帯型電子機器から暗号化および電子署名がなされた前記トランザクションデータを受信すると、前記記憶用公開鍵とペアとなっている記憶用秘密鍵と、前記送信用公開鍵とペアとなっている送信用秘密鍵とを用いて、前記トランザクションデータを復号化する復号化手段と、

復号化された前記トランザクションデータに基づき、決済処理を行う決済処理手段とを有しているカード決済に用いるカード管理装置。

8. 指紋センサ付き携帯型電子機器を、通信端末を介して、カード会社のカード管理装置に接続し、商品購入代金などのカード決済を行うカード決済システムであって、

前記指紋センサ付き携帯型電子機器は、

前記指紋センサにより利用者の指紋を読み取らせ、予め登録されている指紋データと照合することにより、利用者が前記指紋センサ付き携帯型電子機器の所有者であるか否かの本人確認を行う本人確認手段と、

本人確認が行われた場合に、商品注文情報と、予め登録されているカード情報とを、予め登録されている送信用公開鍵によって暗号

化してトランザクションデータを生成すると共に、予め登録されている個人用暗号鍵によって電子署名を行うトランザクションデータの生成・署名手段と、

前記電子署名付きのトランザクションデータを前記カード管理装置に送信する送信手段とを備えており、

前記カード管理装置は、

前記電子署名付きのトランザクションデータを受信する受信手段と、

受信した前記電子署名付きのトランザクションデータを、前記送信用公開鍵とペアとなっている送信用秘密鍵を用いて復号化する復号化手段と、

復号化された前記トランザクションデータに基づき、決済処理を行う決済処理手段とを備えていることを特徴とする指紋センサ付き携帯型電子機器を用いたカード決済システム。

9. 請求の範囲第8項において、

前記指紋センサ付き携帯型電子機器の前記指紋データおよび前記カード情報は、前記カード管理装置の側から付与さた記憶用公開鍵によって暗号化された状態で登録されており、

前記カード管理装置の前記復号化手段は、前記記憶用公開鍵とペアとなっている記憶用秘密鍵を用いて復号化を行うことを特徴とする指紋センサ付き携帯型電子機器を用いたカード決済システム。

10. 請求の範囲第8項または第9項において、

前記カード管理装置は、受信した前記トランザクションデータを所定期間、記憶保持する記憶手段を備えていることを特徴とする指紋センサ付き携帯型電子機器を用いたカード決済システム。

１１．　　請求の範囲第８項、第９項または第１０項において、

前記カード管理装置は、前記指紋センサ付き携帯型電子機器に登録されている前記送信用公開鍵および前記記憶用公開鍵を更新する暗号鍵更新手段を備えており、

前記指紋センサ付き携帯型電子機器は、登録されている前記カード情報および前記指紋データを、更新後の前記記憶用公開鍵を用いて暗号化した前記カード情報および前記指紋データに書き換えるデータ更新手段を備えていることを特徴とする指紋センサ付き携帯型電子機器を用いたカード決済システム。

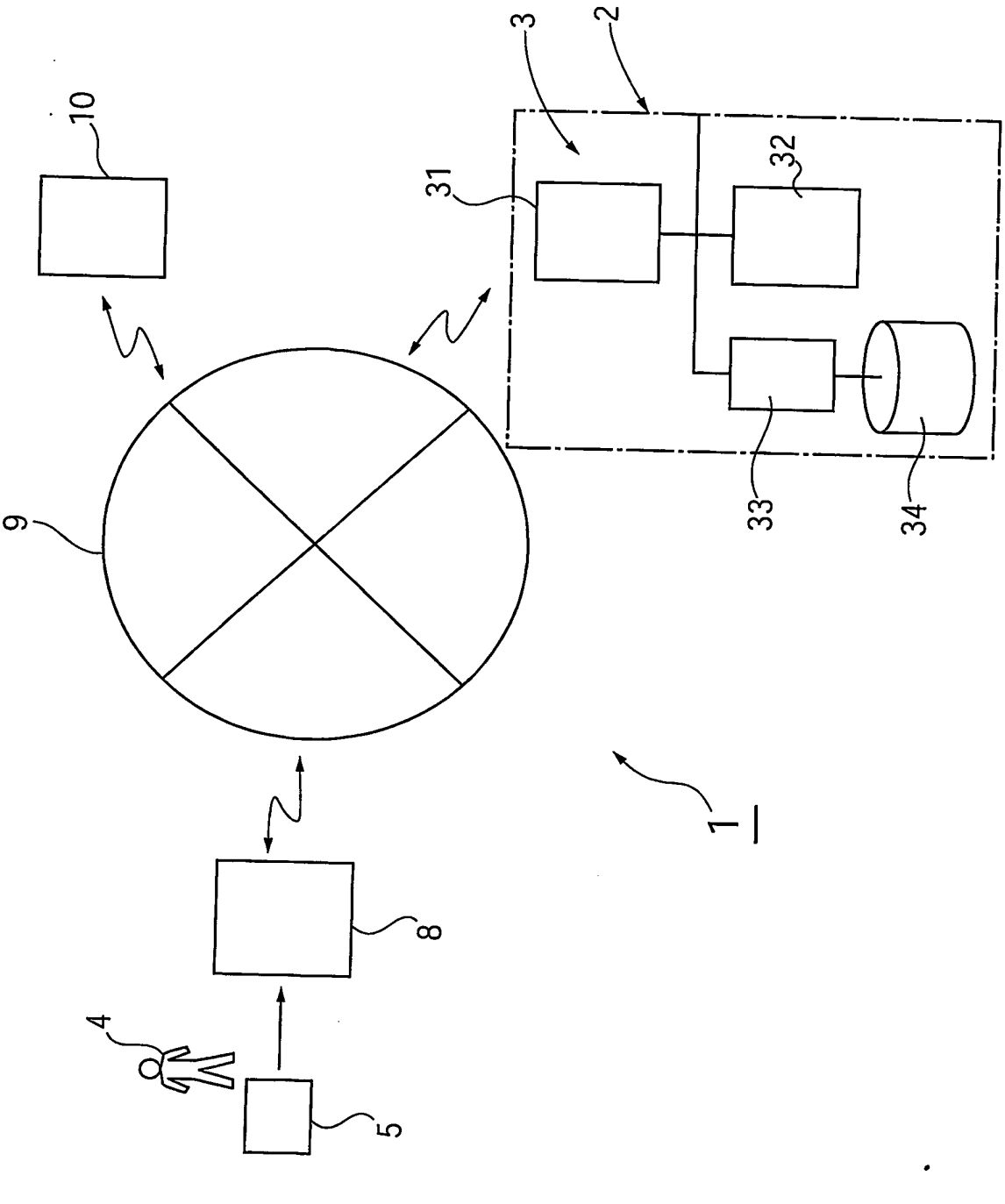


図1

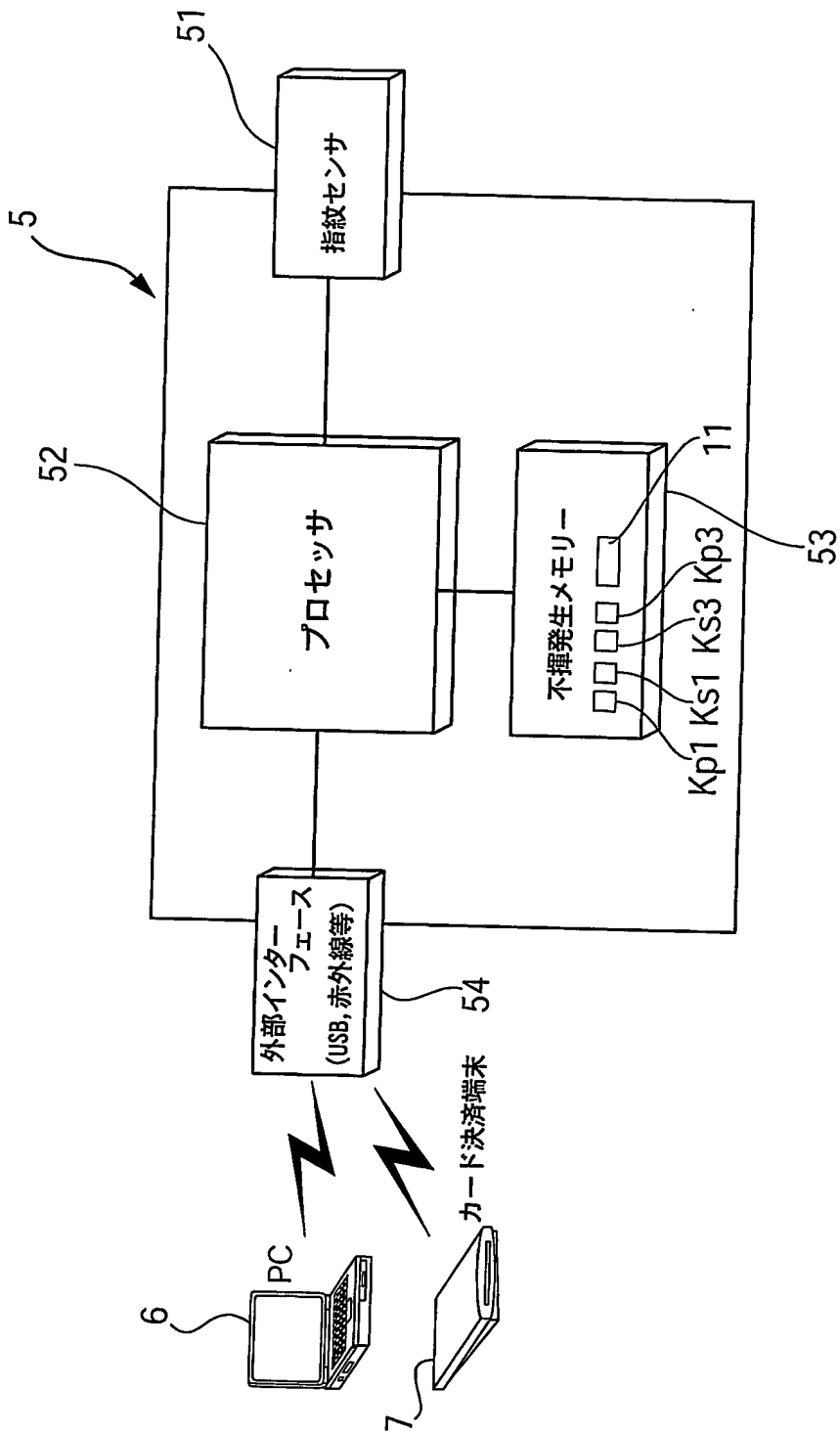

51
指紋センサ
5
52
プロセッサ
不揮発生メモリー
11
53
Kp1 Ks1 Ks3 Kp3
外部インターフェース
(USB, 赤外線等)
54
カード決済端末
PC
6
7

図2

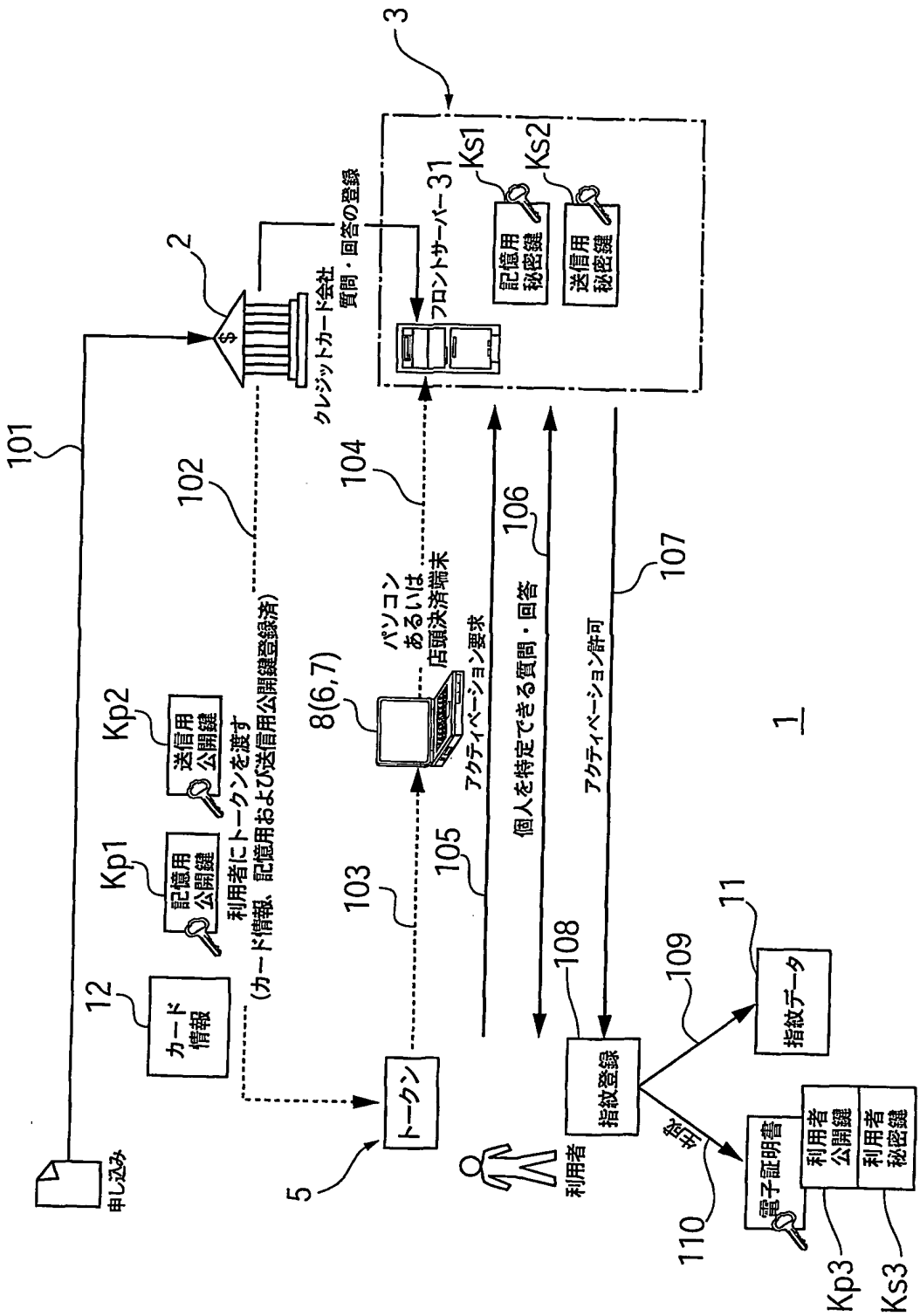

3
2
クレジットカード会社
質問・回答の登録
フロントサーバー 31
Ks1
Ks2
記憶用秘密鍵
送信用秘密鍵
101
102
104
Kp2
送信用公開鍵
Kp1
記憶用公開鍵
利用者にトークンを渡す
(カード情報、記憶用および送信用公開鍵登録済)
8(6,7)
パソコンあるいは店頭決済端末
アクティベーション要求
106
個人を特定できる質問・回答
107
アクティベーション許可
12
カード情報
103
105
108
109
11
指紋データ
申し込み
トークン
5
利用者
指紋登録
1
110
電子証明書
利用者公開鍵
利用者秘密鍵
Kp3
Ks3

図3

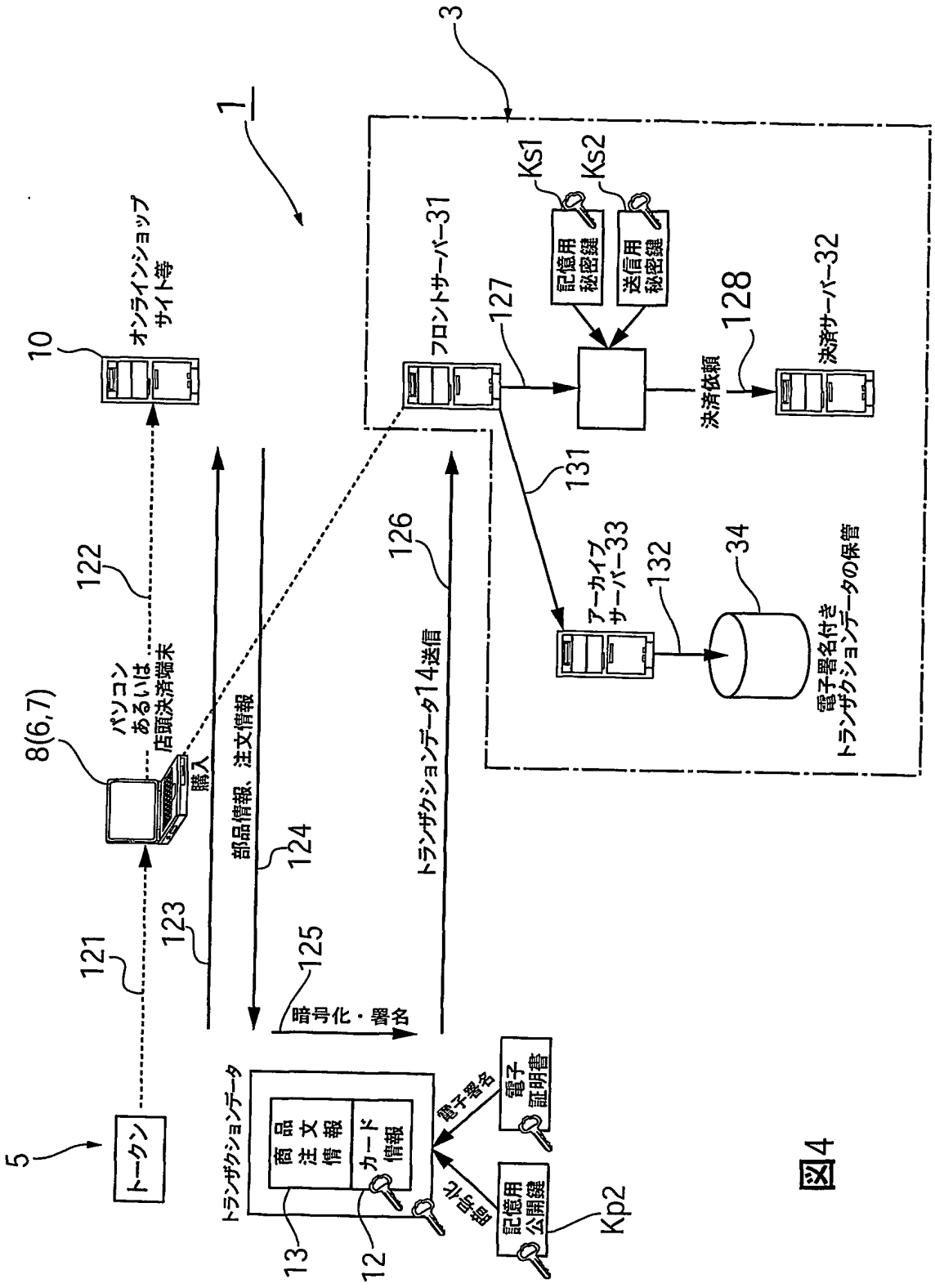

1
3
10
オンラインショップ
サイト等
フロントサーバー31
Ks1
Ks2
記憶用
秘密鍵
送信用
秘密鍵
127
128
決済依頼
決済サーバー32
131
アーカイブ
サーバー33
132
34
電子署名付き
トランザクションデータの保管
126
トランザクションデータ14送信
122
パソコン
あるいは
店頭決済端末
8(6,7)
購入
部品情報、注文情報
124
123
121
125
暗号化・署名
5
トークン
トランザクションデータ
商品
注文
情報
カード
情報
13
12
電子署名
電子
証明書
暗号
記憶用
公開鍵
Kp2

図4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/00473

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2003
Kokai Jitsuyo Shinan Koho 1971-2003 Jitsuyo Shinan Toroku Koho 1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WAHAB, Abdul et al., "Biometrics Electronic Purse", Proceedings of the IEEE Region 10 Conference (TENCON'99), December, 1999, Vol.2, pages 958 to 961, Section "I. INTRODUCTION"	1,3,7,8,10
Y	OPENCARD CONSORTIUM., "OpenCard Framework-General Information Web Document" [online]., 2nd ed., October, 1998, [archival date: 03 June, 2001 (03.06.01)]., retrieved from the Internet Archive (target URL):<URL:http://www.opencard.org/docs/gim/ocfgim.pdf>., Section "Application Tour"	1,3,7,8,10
Y	JP 2001-357371 A (Sony Corp.), 26 December, 2001 (26.12.01), Figs. 2A to 2E (Family: none)	1,3,7,8,10

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 April, 2003 (18.04.03)	30 April, 2003 (30.04.03)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/00473

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2002/0095587 A1 (INTERNATIONAL BUSINESS MACHINES CORP.), 18 July, 2002 (18.07.02), Figs. 5, 6 (Family: none)	1,3,7,8,10
A	JP 2002-132731 A (Hitachi, Ltd.), 10 May, 2002 (10.05.02), Figs. 6, 7 (Family: none)	1-11
A	WO 00/65770 A1 (VERIDICOM, INC.), 02 November, 2000 (02.11.00), Figs. 4, 6 & AU 42501/00 A & EP 1175749 A1 & JP 2002-543668 A	1-11

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０３／００４７３

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.[7]　G06F17/60

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.[7]　G06F17/60

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922–1996年
日本国公開実用新案公報	1971–2003年
日本国登録実用新案公報	1994–2003年
日本国実用新案登録公報	1996–2003年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	WAHAB, Abdul et al. "Biometrics Electronic Purse." *Proceedings of the IEEE Region 10 Conference (TENCON '99)*, 1999.12, pp. (vol. 2) 958–961. *"I. INTRODUCTION" のセクション*	1, 3, 7, 8, 10
Y	OPENCARD CONSORTIUM. "OpenCard Framework — General Information Web Document" [online]. 2nd ed., 1998.10 [archival date: 2001.06.03]. retrieved from the Internet Archive (target URL):	1, 3, 7, 8, 10

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 18.04.03	国際調査報告の発送日 30.04.03
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 阿波　進　5L　9168 電話番号　０３－３５８１－１１０１　内線　３５６１

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
	<URL: http://www.opencard.org/docs/gim/ocfgim.pdf>. *"Application Tour" のセクション*	
Y	JP 2001-357371 A (ソニー株式会社) 2001.12.26 *図 1; 2A–2E* (ファミリーなし)	1, 3, 7, 8, 10
Y	US 2002/0095587 A1 (INTERNATIONAL BUSINESS MACHINES CORP.) 2002.07.18 *図 5, 6* (ファミリーなし)	1, 3, 7, 8, 10
A	JP 2002-132731 A (株式会社日立製作所) 2002.05.10 *図 6, 7* (ファミリーなし)	1–11
A	WO 00/65770 A1 (VERIDICOM, INC.) 2000.11.02 *図 4, 6* & AU 42501/00 A　& EP 1175749 A1　& JP 2002-543668 A	1–11